ivanti

Informe de Ciberseguridad del Consumidor 2021:

Cómo el teletrabajo expone a las empresas ante el riesgo de un ciberataque

El comportamiento de consumo arriesgado está debilitando la ciberseguridad

La pandemia de 2020 no sólo desató un virus mortal y devastador en todo el mundo, sino que también alteró fundamentalmente todos los aspectos de nuestra vida cotidiana, incluido dónde y cómo se trabaja. Siempre que fuera posible, trabajadores de todos los sectores empezaron a teletrabajar. Aunque las fuerzas de trabajo remotas ayudaron a que las operaciones importantes de las empresas siguieran adelante, muchas organizaciones se enfrentan ahora a un preocupante aumento de las amenazas de ciberseguridad, debido a la afluencia de dispositivos personales inseguros y al comportamiento arriesgado de los empleados. Tras más de un año de pandemia, ¿cómo es actualmente el panorama de las amenazas?

El pasado mes de febrero, Ivanti ha publicado el "Informe de Ciberseguridad del Usuario 2021", que revela las amenazas concretas que ponen en riesgo a las empresas. Los resultados se basaron en una muestra representativa a nivel nacional de más de 2.000 personas mayores de 18 años que trabajaban en Estados Unidos y el Reino Unido en noviembre de 2020.

Aunque las organizaciones han sido conscientes de las vulnerabilidades que plantean los dispositivos y aplicaciones no gestionados propiedad de los empleados, este informe ha revelado que los empleados tienen comportamientos de alto riesgo incluso cuando se les dan ordenadores de la empresa para teletrabajar. Por ejemplo, uno de cada cuatro consumidores ha admitido haber utilizado su correo electrónico o contraseña del trabajo para acceder a sitios web y aplicaciones de consumo, como aplicaciones de entrega de alimentos, sitios de compras en línea e incluso aplicaciones y páginas de citas.

Obstaculizar la seguridad empresarial

Even Aunque el mundo acabe volviendo a la "normalidad" previa al COVID, es probable que el teletrabajo permanezca. Aunque las organizaciones han tratado de suplir las carencias de seguridad de sus trabajadores a distancia, es evidente que tendrán que hacer algo más que proporcionar hardware y software de propiedad de la empresa. Un examen más detallado de las conclusiones del informe, debería dar a las empresas una mejor visión de los retos que tienen por delante.

1 de cada 4 consumidores

admiten que utilizan su correo electrónico o contraseña del trabajo para acceder a sitios web y aplicaciones de consumo, como aplicaciones de entrega de alimentos, sitios de compras online e incluso aplicaciones y páginas de citas.

Los hábitos de seguridad de los empleados a distancia ponen en peligro a sus empresas

Para entender mejor el nivel de seguridad del entorno medio de trabajo desde casa, la encuesta ha consultado a los encuestados sobre su comportamiento y prácticas de seguridad para todos sus dispositivos, incluidos los dispositivos IoT en el hogar.

Credencias recicladas:
Casi una cuarta parte de los encuestados en Estados Unidos y casi uno de cada cinco en el Reino Unido, afirmaron haber utilizado su correo electrónico o contraseña del trabajo para iniciar sesión en sitios web y aplicaciones de consumo.

Dispositivos personales para trabajar:
Casi la mitad de los encuestados de Estados Unidos y más de un tercio de los del Reino Unido, dijeron que se les permite utilizar un dispositivo personal, como un ordenador portátil, un teléfono inteligente, una tableta o un reloj inteligente para acceder a las aplicaciones y redes de la empresa.

Autenticación de dos factores para dispositivos IoT:
Casi la mitad de los encuestados de Estados Unidos y el Reino Unido no han configurado la autenticación de dos factores para los dispositivos inteligentes en sus hogares.

Los puntos clave a tener en cuenta: no olvidar las prácticas básicas de seguridad en casa.

La falta de salvaguardias básicas de seguridad en todos los dispositivo IoT del hogar, deja tanto a los trabajadores remotos como a sus empresas más vulnerables frente a las ciberamenazas, como el hackeo de las cámaras de seguridad de Ring, que se hizo viral en 2019.

Los malos hábitos de seguridad, como reciclar las contraseñas para acceder a los sitios web de los consumidores, pueden hacer que las empresas corran un mayor riesgo de sufrir una infracción. Las organizaciones deben imponer una clara separación entre las aplicaciones y los sitios web utilizados para el trabajo y los asuntos personales.

La seguridad de las empresas también es limitada entre los trabajadores a distancia

Tras el inicio de la pandemia, vimos un preocupante aumento de los ataques de ciberseguridad contra dispositivos personales inseguros y dispositivos IoT en el hogar. Aunque los malos hábitos de seguridad de los usuarios finales pueden tener parte de culpa, nuestra encuesta ha revelado que las empresas también pueden mejorar la seguridad en áreas clave.

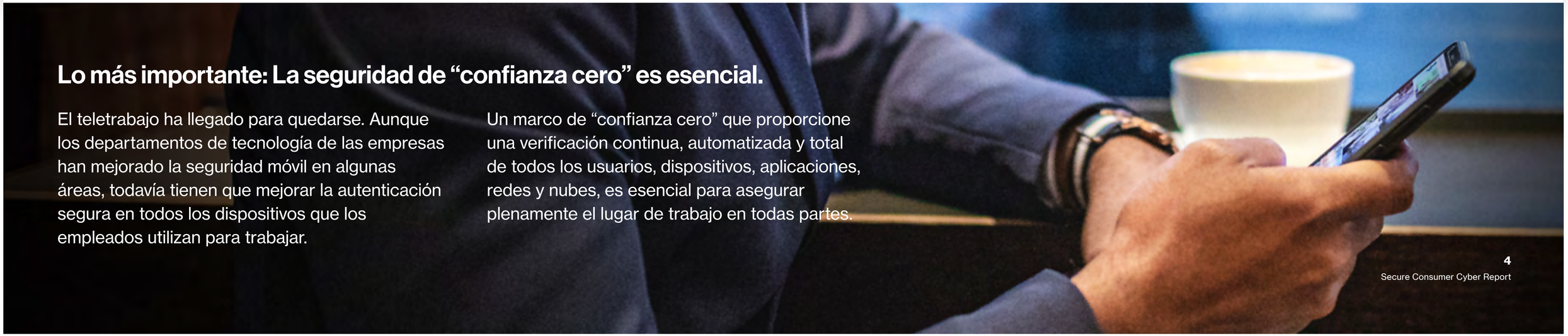
25%

Software de seguridad:
Más de una cuarta parte de todos los encuestados,consideraban que no estaban obligados a tener un software de seguridad específico en sus dispositivos para acceder a ciertas aplicaciones mientras trabajan a distancia.

Actualización de la contraseña:
Aproximadamente el 25 % de los trabajadores remotos de EE.UU. y el Reino Unido, afirmaron que su empresa no les exige que actualicen su contraseña cada seis meses o que utilicen un generador de contraseñas de un solo uso.

30%

Herramientas de acceso seguro:
Casi el 30 % de todos los encuestados en Estados Unidos y el Reino Unido, dijeron que su organización no exige a los trabajadores remotos que utilicen una herramienta de acceso seguro, como una VPN.



Lo más importante: La seguridad de “confianza cero” es esencial.

El teletrabajo ha llegado para quedarse. Aunque los departamentos de tecnología de las empresas han mejorado la seguridad móvil en algunas áreas, todavía tienen que mejorar la autenticación segura en todos los dispositivos que los empleados utilizan para trabajar.

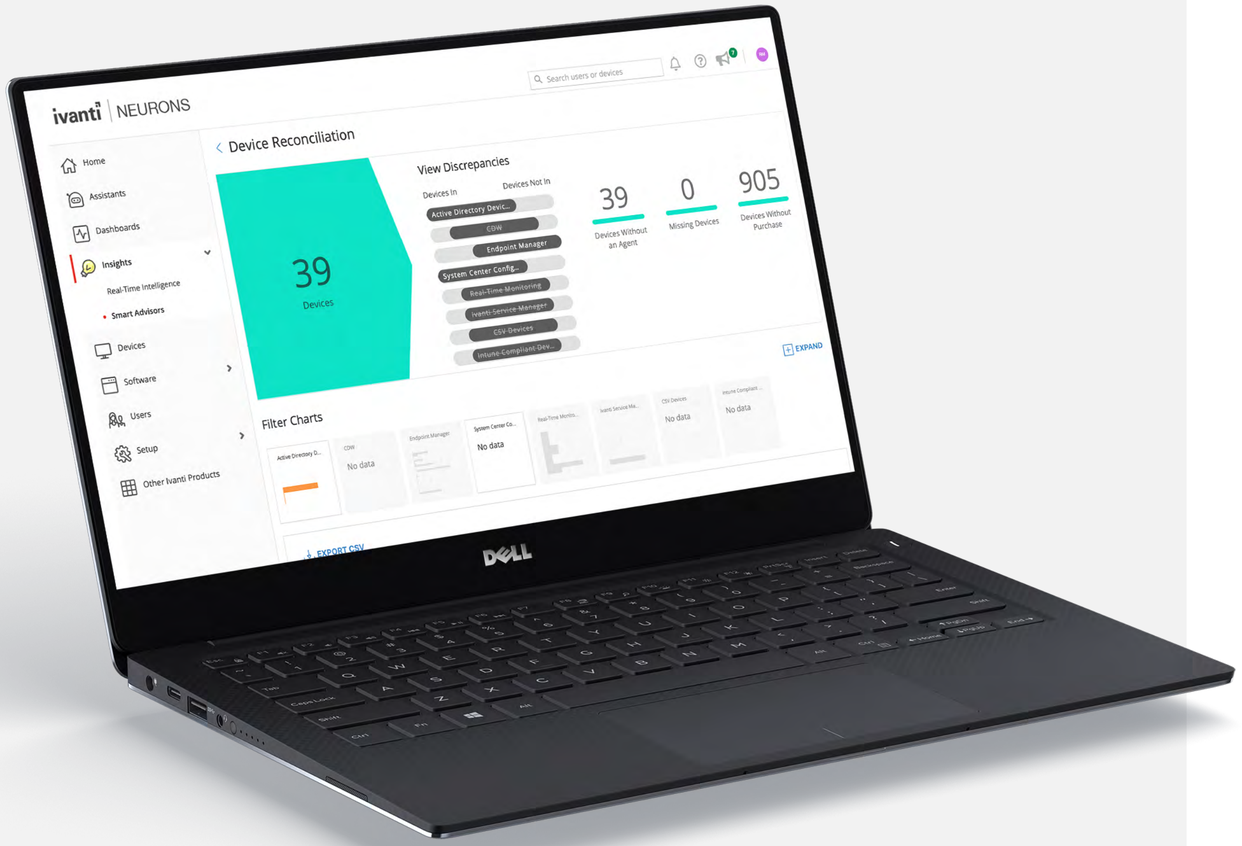
Un marco de “confianza cero” que proporcione una verificación continua, automatizada y total de todos los usuarios, dispositivos, aplicaciones, redes y nubes, es esencial para asegurar plenamente el lugar de trabajo en todas partes.

La seguridad de los usuarios es la la seguridad de las empresas

Con más gente que nunca trabajando a distancia, el panorama de las amenazas se ha ampliado más rápido que nunca. Por ello, las empresas deben buscar estrategias clave para salvaguardar las aplicaciones y los datos de la entidad contra los fallos de seguridad del IoT, y también para proteger a los usuarios cuando trabajan desde casa.. Está claro que a medida que se emplean más dispositivos de consumo, los trabajadores remotos pueden tener dificultades para activar y mantener la configuración de seguridad avanzada, y los ciberdelincuentes lo saben. Como resultado, además de crear una amenaza masiva para la salud humana, la pandemia causada por el COVID-19 también ha puesto en riesgo nuestro bienestar, al facilitar que los ciberdelincuentes se aprovechen de las personas y organizaciones que carecen de la protección adecuada.

Sin embargo, hay buenas noticias: las empresas pueden poner en marcha hoy mismo la seguridad de “confianza cero”

Las organizaciones pueden actualmente tomar medidas para empezar a implementar protocolos de “confianza cero” en toda la estructura de trabajo a distancia. Con un modelo de “confianza cero”, las empresas podrán eliminar el riesgo de robo de credenciales verificando que cualquiera que acceda a la información, las aplicaciones o las redes corporativas, sea una entidad de confianza. Además, a medida que el trabajo remoto persiste y los dispositivos siguen proliferando, la seguridad de “confianza cero” puede facilitar mucho la aplicación de políticas de uso aceptable, incluido el uso de la autenticación multifactor, las protecciones de los dispositivos y la conectividad de red segura.



Metodología

Las conclusiones del primer Informe sobre Ciberseguridad del Consumidor se basan en una encuesta realizada en noviembre de 2020. El estudio se ha diseñado para examinar cómo han cambiado los hábitos de ciberseguridad de los consumidores y las empresas en el transcurso de la pandemia. La encuesta utilizó una muestra representativa a nivel nacional de 2.000 residentes de Estados Unidos y Reino Unido mayores de 18 años que teletrabajan con un ordenador proporcionado por la empresa.

Sobre Ivanti

La plataforma de automatización de Ivanti hace que cada conexión informática sea más inteligente y segura a través de los dispositivos, la infraestructura y las personas. Desde los ordenadores y los dispositivos móviles hasta la infraestructura del escritorio virtual y el centro de datos, Ivanti descubre, gestiona, asegura y da servicio a los activos de TI desde la nube hasta el borde de la empresa omnipresente (que está “en cualquier lugar”), mientras que ofrece experiencias personalizadas a los empleados. En el trabajo omnipresente, los datos corporativos fluyen libremente por los dispositivos y servidores, lo que permite a los trabajadores ser productivos dondequiera y comoquiera que trabajen. Ivanti tiene su sede en Salt Lake City, Utah, y cuenta con oficinas en todo el mundo. Para más información: www.ivanti.com y siga a @GoIvanti.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com